PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-211147
(43)Date of publication of application : 03.08.2001

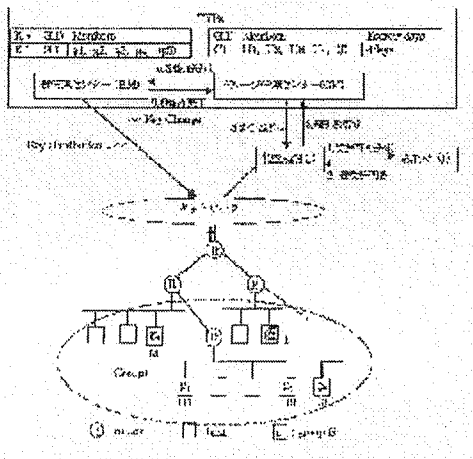
(51)Int.Cl. H04L 9/08
G09C 1/00

(21)Application number : 2000-015240
(22)Date of filing : 25.01.2000

(71)Applicant : ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
(72)Inventor : INOUE TORU
BOKU BIJIYOU
KURIHASHI SHINJI

(54) KEY ESCROW METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To constitute a cipher key deposit system at low cost and to shorten the time up to the start of an interception by an investigation agency.
SOLUTION: A key deposit agent is provided for a group cipher communication system which conduct a cipher communication by using a group session key. When the key deposit agency generates and distributes the group session key to form a communication group, a dummy user is registered as a member of the communication group. For investigation, a dummy user of a communication group as an object of interception is assigned to the investigation agency and a cipher communication is intercepted and deciphered. The cipher communication of the communication group can speedily be intercepted when necessary in investigation and even if the group member constitution changes, the investigation agency is included as a group member only in the communication group including an object person to be investigated, so that the cipher communication can securely be intercepted.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the key escrow method of making an encryption key for a criminal investigation agency to decode an encryption message for the purpose of a criminal investigation depositing, about the key escrow method.
[0002]
[Description of the Prior Art]Methods of making the encryption key in the conventional cipher communication system depositing include the art of the Clipper Chip method. This is used when the American government monitors for the purpose of a criminal investigation. the tamper beforehand instrumentated to telephone etc. -- the conversation of a telephone is enciphered by the resist Clipper Chip. The key information used for the encryption at that time is recorded on a kind of header called LEAF (Law Enforcement Access Field). The contents of LEAF serve as the 80-bit session key Ks and the device inherent key Kui of the 32-bit device i from a total of 128 bits of the 16-bit checksum Check, as shown in drawing 4.
[0003]The device inherent key of the Clipper Chip which a user uses is beforehand divided and deposited with two key depository institutions. Although this key is kept secretly, when it is judged from the necessity on judicial-affairs execution that the decipherment of a code is required, a criminal investigation agency can ask each key depository institution for delivery of a key, after acquiring permission of a court.
[0004]When a criminal investigation agency monitors communication, session key information is restored and extracted from **LEAF decoder using key Kr. ** A criminal investigation agency sends the taken-out device identifier Di to two key depository institutions. ** The key depository institutions 1 and 2 search Di to Kui^1, and Kui^2, and calculate Kui^1 and Kui^2, respectively. ** Send Kui^1 and Kui^2 to a criminal investigation agency. ** Compound Kui^1 and Kui^2 which

came to hand from the key depository institutions 1 and 2, and restore the session key Ks. The cryptogram which this monitored is decoded. While decentralizing a key depository institution for the prevention from conspiracy, in order to prevent unrestricted interception, he is trying not to pass a criminal investigation agency a key directly.

[0005]Here, the conditions required of a key escrow system are explained. In order to monitor communication with a criminal investigation agency etc. about permission of interception, the interception permit from a court defined from the country must be received. About data restoration, decoding to a plaintext from a cryptogram must be performed using an encryption key. In order to protect a user's privacy, unrestricted interception of a criminal investigation agency must be prevented.

[0006]The key escrow framework must give a lawful user profits. Of course between international, domestic must enable offer of key escrow service. It is necessary to place the independent organization (TTPs: Trusted Third Parties) which was exhibited by the public and which is trusted. The art known well must be used for realization of TTPs. It is not limited to a specific communication configuration, but all the telecommunication gestalten must be supported. The criminal investigation agency has to enable it to access real time, if interception permission is obtained. Restriction must be given at the time when a key is used. In realization, although it is hardware, probably it is software, but it must not be dependent on a certain specific cryptographic algorithm. It must be made impossible that a criminal investigation agency draws up a fake interception license form.

[0007]By the way, the multicast router in which the multicasting routing protocol is mounted is being realized. Operation of IGMP defined on the Internet currently built by the multicast router as a protocol which performs group management between host routers has the following features. Each group is identified by one IP address. A group's scale is arbitrary. A group's member may be in the arbitrary places on the Internet. A group's member can do secession from the intervention and the group to a group always (receiver-oriented).

[0008]In a large-scale network system, these features are dramatically convenient, in order to perform group communication efficiently. However, about the point that it is a protocol [receiver-oriented / last], everyone only joins a group address and has a big problem from a viewpoint on the security that a multicast packet will be receivable. For example, in the contents distribution service accompanied by fee collection, etc., it may throw a furtive glance at contents for nothing in addition to a registered member. There is also a problem that persons other than a group's member can transmit a multicast packet. In order to solve such a problem and to take care of a well-intentioned user, it is necessary to perform encryption group communication.

[0009]As the technique of building group communication in a code, as shown in drawing 5, there are a path definition method and an area definition method. In the path definition method

shown in drawing 5 (a), a different session key for every pair of a group member is held, and a group administrator manages them all. A session key is exchanged among the group members who communicate at the time of the start of a communication session. In this method, although construction of a flexible system is possible by having a key with which all the communication paths differ, the load of management of a session key is large and is limited to a small-scale system.

[0010]On the other hand, in the area definition method shown in drawing 5 (b), a common session key is shared among group members. The session key is beforehand distributed to timing independent of a communication session. Management of a session key is easy for this method, and can apply it also to a large-scale system. In the group communication by an area definition method, it is necessary to update a session key periodically from a viewpoint of security. Also when a group's composition changes, renewal of a session key is needed.

[0011]It is necessary to take care of a lawful user by performing encryption group communication on the Internet currently built by such multicast router. In order to prevent abusing such a cipher communication system with it, it is necessary to introduce the key escrow system which enables interception by governmental authority.

[0012]As conventional key escrow methods other than the Clipper Chip method, For example, R. Ganesan:"Yaksha:Augmenting. Kerberos with Public Key Cryptography, "Proc. ISOCSymp.on Network and Distributed System Security, and Feb.1995., Yamane Whether they are Yoshinori and Koichi Sakurai:"key escrow method which prevents unrestricted tapping" Proc. SCIS96, and Feb.1996., and quantity Taniwa ** and the Ogata **, There are some which are proposed by Hitoshi Sakagami and Takahashi **:"key escrow method which protects privacy" Proc. SCIS99, pp.905-910, Feb.1999., etc.

[0013]

[Problem(s) to be Solved by the Invention]However, in the above-mentioned Clipper Chip method, since key information was taken out, two organizations were requested, the key was compounded and the session key was taken out from LEAF after obtaining permission, there was a problem that it surely took 2 hours or more. a tamper -- in order to be dependent on resist hardware, there was a problem that expense also started. There was a problem that interception might be escaped, by attaching fake LEAF.

[0014]This invention solves the above-mentioned conventional problem, and an object of this invention is for a criminal investigation agency to enable it to monitor certainly by low cost for a short time at the time of criminal investigation in the key escrow method of a group cipher communication system.

[0015]

[Means for Solving the Problem]In order to solve the above-mentioned technical problem, in this invention, a key escrow method of a group cipher communication system of performing

encryption communication using a group session key, When carrying out generation distribution of the group session key in a key escrow organization and forming a communication group, a straw-man user was registered as a communication group's member, and at the time of criminal investigation, a straw-man user of a communication group for interception was assigned to a criminal investigation agency, and it had composition of monitoring and decoding encryption communication.

[0016]By having constituted in this way, when required of criminal investigation, interception of a communication group's encryption communication is attained in an instant. In a communication network where a group member is changed dynamically, however group member composition may have change, only a communication group in whom a criminal-investigation candidate is contained can do interception of encryption communication certainly only by including a criminal investigation agency as a group member.

[0017]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail, referring to drawing 1 - drawing 3.

[0018]An embodiment of the invention is the key escrow method of registering a straw-man user as a communication group's member, and monitoring by assigning a criminal investigation agency a straw-man user at the time of criminal investigation, when carrying out generation distribution of the group session key in a key escrow organization and forming a communication group.

[0019]Drawing 1 is a key map showing the procedure of the key escrow method in an embodiment of the invention. In drawing 1, TTPs (Trusted Third Parties) is a lock management organization which provides key escrow service. A group management center (GM) is an organization which manages a group member. A lock management center (KM) is an organization which updates a session key periodically while distributing the session key to each group. Criminal investigation agency (I) is a criminal investigation agency which gets interception permission and gets a key from TTPs. A court (J) is a court which publishes an interception license form.

[0020]Drawing 2 is a figure showing the group session key share sequence of the key escrow method in an embodiment of the invention. In drawing 2, KM is a lock management center. GM is a group management center. g1 -- gi-- is a group member. g5 is a terminal of a criminal investigation agency.

[0021]Drawing 3 is a figure showing the key delivery sequence of the key escrow method in an embodiment of the invention. In drawing 3, KM is a lock management center. GM is a group management center. I is a criminal investigation agency. J is a court.

[0022]The example applied to the group communication on the Internet explains the operation procedures of the key escrow method in the embodiment of the invention constituted as

mentioned above. In order to solve the security issue of IP multicast communication and to realize safe group communication, multicast group encryption communication is realized by using the network structure of the existing IP multicast as it is, and giving a cryptographic function to the terminal side. This group cipher key deposit method provides the service which protects a system from what abuses such multicast group encryption communication. According to this embodiment, group encryption communication by an area definition method is set as the object of a key escrow.

[0023]The key escrow model (KSM:Key Escrow Model) of group encryption communication is defined as follows.

[Definition] KSM= (TTPs, I, G)

Here, TTPs (Trusted Third Parties) is a lock management organization which provides key escrow service according to a demand and which is trusted. The group management center (GM:Group Management Center) where this manages a group member, Regardless of a member's personal information, the session key to each group is distributed and it comprises a lock management center (KM:Key ManagementCenter) which updates a key periodically. I (Interception Agency) is a criminal investigation agency which gets the interception permission for decoding the monitored cryptogram, and gets a key from a lock management organization (TTPs). G (secure Communication Groups) is the group who comprised a user who wishes group encryption communication on an IP multicast communication plat form.

[0024]In the key escrow system of the group encryption communication shown in drawing 1, each organization has the public key Px and the secret key Sx, respectively (x=gi, GM, KM, I, J). Communication between a group's users is performed by the common key encryption system.

[0025]A user (U:User) is a user who joins a key escrow system and performs encryption communication. Each user has user names (U1 etc.) and host names (g1 etc.). Two or more communication groups G may exist as a group who comprises a user who wishes group encryption communication. The user can participate in the encryption communication between two or more groups.

[0026]The group management center (GM:Group Management Center) has managed the personal information of the user who wishes group encryption communication. A group management center (GM) registers each group member. The interception license form from the court (J) which permits the interception to a certain group, Without obtaining permission of a member addition from the group member, if shown from criminal investigation agency (I), it registers as a group member from whom criminal investigation agency (I) was hidden, and a key distribution request is carried out to a lock management center (KM).

[0027]A lock management center (KM:Key Management Center) generates the session key (Ks) used by group encryption communication, and distributes and updates a session key

periodically according to the key distribution request from a group management center (GM) to a member. A lock management center (KM) understands only each user's host name requested from a group management center (GM). Therefore, also when criminal investigation agency (I) goes into a group, existence of a criminal investigation agency comes to distribute a session key, not known.

[0028]A criminal investigation agency (I:Interception Agency) is the criminal investigation purpose, and are interception of group communication, and an organization which decrypts the monitored cryptogram. A court (J:Court of Justice) is an organization which attests a criminal investigation agency and takes out an interception-of-communications license form as what it is legally set and can be trusted from a country. In order to protect a user's privacy, the interception license form which set the interception period is published.

[0029]The share procedure of a group session key is explained with reference to drawing 1 and drawing 2. The session key share procedure for performing group encryption communication consists of the group recording step, a key distribution step to a group member, and a periodical session key renewal step as follows.

[0030]STEP1: When the users which wish group registration (1-1) group encryption communication create a group member list (GL) and they transmit each member's public key (Pgi) to the group management center (GM) of a lock management organization (TTPs), request group registration. The user (U1-U4) who shows drawing 1 forms the group 1, and sends (U1, U2, U3, U4) to a group management center (GM) with key information as a group member list (GL).

[0031](1-2) A group management center (GM) assigns G1 to the group member list (GL) as a group identification descriptor (GID), performs member registration, and transmits a user's host name (gi) and public key (Pgi) to a lock management center (KM). A group management center (GM) sets up a straw-man user for criminal investigation agencies. When not monitoring communication, a group management center (GM) keeps a straw-man user's information. When monitoring communication, ID(I) of a criminal investigation agency is assigned, member registration is performed, and the user's I host name (g5) and public key (Pg5) are transmitted to a lock management center (KM).

[0032]In the example shown in drawing 1, a group management center (GM) assigns and registers the group identification descriptor G1 into a group member list (U1, U2, U3, U4). A user's host name (g1-g4) and public key (Pg1-Pg4) are transmitted to a lock management center (KM).

[0033](1-3) A lock management center (KM) assigns a multicast address (MA) about the group member list received from the group management center (GM). At this time, a lock management center (KM) also assigns a straw-man user or a criminal investigation agency a multicast address (MA).

[0034]STEP2: Session key distribution (2-1) gi->GM:DIS_REQ (G1)
To be shown in drawing 2, the member (gi) of the encryption communication group who performed group registration in the group management center (GM) gives G1 of group ID to a group management center (GM), sends a distribution request, and requests session key distribution.
[0035](2-2) GM->KM:DIS_REQ (G1, GL)
A group management center (GM) gives group ID and a group member list (GL) to a lock management center (KM), sends a distribution request, and requests session key distribution in a group.
[0036](2-3) A KM->G:KEY_DIS[G1, K1, time-exp] Pgi lock management center (KM), The check of registration group ID and the group member list GL is performed, as a session key with the term of validity (Ks), it enciphers to each member by each user's public key (Pgi), and K1 is distributed to him by a unicast. This session key (K1) shall not be used if the term of validity passes.
[0037](2-4) gi->KM:K_ACK (gi)
By decoding with its own secret key (Sgi), each member (gi) of the group who received the session key with the term of validity (K1) returns a session key received response to a lock management center (KM).
[0038](2-5) KM->GM:DIS_ACK (G1, GL)
If session key received responses are received from all the members, a lock management center (KM) will send a session key distribution completion notification to a group management center (GM).
[0039]STEP3 : a renewal (3-1) KM->Gof session key:[KEY_CHA] K1 lock-management center (KM), A session key update message (KEY_CHA) is enciphered to the group's G1 multicast address (MA) with the session key K1 used now, and it transmits to it all at once by an IP multicast.
[0040](3-2) gi->KM:CHA_ACK (gi)
Each member (gi) sends the renewal Acknowledgement message of a session key to a lock management center (KM).
[0041](3-3) A lock management center (KM) redistributes the new session key to the group G1 according to (2-3) of STEP2, and (2-4). This is performed periodically.
[0042]The procedure of key delivery for a criminal investigation agency to monitor group encryption communication with doubt of a crime with reference to drawing 3 is explained.
When a criminal investigation agency wants to monitor the encryption communication of a group with the possibility of a certain crime, I have to get a court to publish an interception license form. In order to attest a criminal investigation agency, the criminal investigation agency which can monitor is beforehand registered into the court.

[0043]STEP1: Interception permission demand 1.I->J:ESC_REQ (I, G1)
Criminal investigation agency (I) attaches I which is its ID, and G1 which is the names of the criminal group who wants to monitor, sends an interception demand, and requires interception license form issue of a court (J).
[0044]STEP2: Interception license form issue 2.J->I:ESC_PER ($[K_{I, GM}, [LJ]_{KGM}]_{KI}$)
A court (J) attests criminal investigation agency (I), and if it is a right criminal investigation agency, it will publish the interception license form with a certificate (LJ) which defined an interception shelf-life (Days) and group ID. This license form is enciphered with the common key KGM with the group management center (GM). Common key $K_{I, GM}$ which can be used between criminal investigation agency (I) and a group management center (GM) are also prepared. This is enciphered with the common key KI with criminal investigation agency (I), and it sends to criminal investigation agency (I).
[0045]STEP3: Key delivery demand 3.I->GM:KEY_ESC_REQ ($[A.I. Artificial Intelligence]_{KI, GM}$, $[LJ]_{KGM}$)
Criminal investigation agency (I) decodes the encipherment information sent from a court (J), and takes out a common key ($K_{I, GM}$) and an interception license form (LJ) with a group management center (GM). And its certification information (A.I. Artificial Intelligence) is created, [who described the time stamp at the time of his ID(I), a secret key, a host address (g5), and message preparing] This is enciphered with a common key ($K_{I, GM}$) with a group management center (GM), and it sends to a group management center (GM).
[0046]
STEP4:key delivery permission 4.GM->I:KEY_ESC_ACK (G1, Days)
After a group management center (GM) checks the certification information of the interception license form (LJ) which the court (J) published, and a criminal investigation agency, Criminal investigation agency (I) is added to the group member of the group G1 for interception, the interception term of validity is set up with a timer device, and the Acknowledgement in which the interception during an interception period is possible is shown in criminal investigation agency (I).
[0047]STEP5: Group session key distribution-request 5.GM->KM:DIS_REQ (G1, g5)
A group management center (GM) tells a lock management center (KM) about the host address (g5) of group ID and the group member I, and it requests session key distribution to the host.
[0048]STEP6: A group session key distribution 6.KM->g5:KEY_DIS[G1, K1, time-exp] PI lock management center (KM) adds a host (g5) to the group G1, and gives the group's multicast address (MA). And the session key (K1) used now is enciphered and sent by the public key

(PI) of criminal investigation agency (I) into the group. Criminal investigation agency (I) to which I had the session key (K1) sent serves as a group's member, by receiving a multicast communication packet, to group encryption communication, becomes accessible to real time and can be monitored. When performing a group's renewal of a key in the lock management center (KM), new key distribution is performed to addressing to a member of G1 which added the registration host (g5) of criminal investigation agency (I).

[0049]STEP7: Criminal investigation agency exclusion 7.GM->KM:DEL_REQ (G1, g5)
By the timer settings of a group management center (GM), after an interception period expires, it is required from a group management center (GM) that the registration host (g5) of a criminal investigation agency should be removed from the group's G1 member to a lock management center (KM).

[0050]STEP8: Criminal investigation agency exclusion check 8.KM->GM:DEL_ACK (G1, g5)
A lock management center (KM) sends an exclusion check to a group management center (GM), after removing the registration host (g5) of a criminal investigation agency from the group's G1 member. Thus, unrestricted interception of the group communication of a criminal investigation agency can be prevented.

[0051]The privacy of user's information is explained. Since a user's user name and group name about personal information, and terminal host name, and secret key information are separated and kept, a user's information cannot be known other than TTPs. Since a court attests a criminal investigation agency and enciphers and hands an interception license form with an interception period with the common key of a court and a group management center, the criminal investigation agency cannot alter it. Since a group management center (GM) attests a criminal investigation agency and the lock management center (KM) is told only about the host name of a criminal investigation agency, unless a group management center (GM) and a lock management center (KM) conspire, the lock management center (KM) cannot know existence of a criminal investigation agency.

[0052]As mentioned above, when carrying out generation distribution of the group session key for the key escrow method in a key escrow organization and forming a communication group in an embodiment of the invention, Since it was considered as the method of registering a straw-man user as a communication group's member, and monitoring by assigning a criminal investigation agency a straw-man user at the time of criminal investigation, When the character of a multicast group management protocol is used and a criminal investigation agency becomes a group's member in consideration of an IP multicast communication plat form, it is accessible to real time in the group encryption communication to which renewal of a key is carried out dynamically. The user using the Internet can always be supervised and can be protected from what abuses a system, and the user can enjoy various services now in comfort.

[0053]
[Effect of the Invention]So that clearly from the above explanation in this invention. The key escrow method of a group cipher communication system of performing encryption communication using a group session key, When carrying out generation distribution of the group session key in a key escrow organization and forming a communication group, register a straw-man user as a communication group's member, and at the time of criminal investigation. Since it had composition of having assigned a criminal investigation agency the straw-man user of the communication group for interception, and monitoring and decoding encryption communication, When required of criminal investigation, interception of a communication group's encryption communication is attained promptly, a criminal investigation agency is only included only in the communication group in whom a criminal-investigation candidate is contained even if group member composition has change as a group member, and the effect that interception of encryption communication can be performed certainly is acquired.
[0054]For a user, since a key escrow organization is a reliable service provision organization, group registration can be performed in comfort.

[Translation done.]

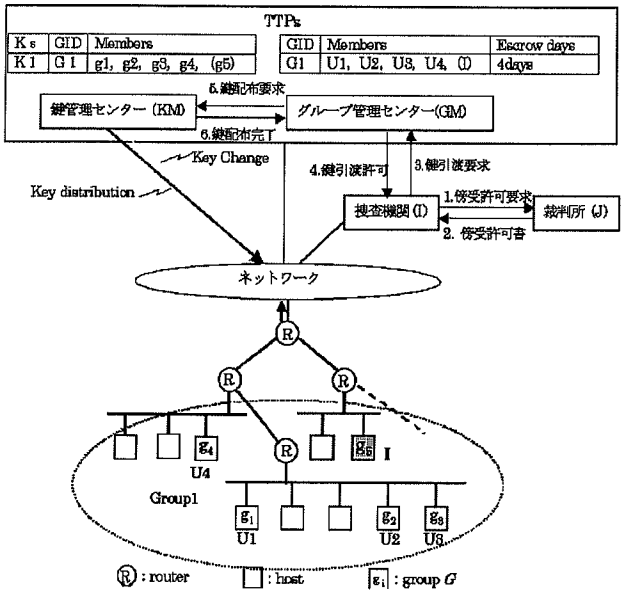
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]In a key escrow method of a group cipher communication system of performing encryption communication using a group session key, When carrying out generation distribution of said group session key in a key escrow organization and forming a communication group, register a straw-man user as said communication group's member, and at the time of criminal investigation. A key escrow method assigning a criminal investigation agency a straw-man user of a communication group for interception, and monitoring and decoding encryption communication.
[Claim 2]A key escrow method according to claim 1, wherein said key escrow organization cancels said straw-man user's assignment to said criminal investigation agency after an end of an interception term and eliminates said criminal investigation agency from said communication group.
[Claim 3]Provide a group management center and a lock management center which carried out mutually-independent in said key escrow organization, and said group management center, If said criminal investigation agency checks an interception license form which received from a court, said criminal investigation agency will be added to said interception object communication group's member by assigning said criminal investigation agency an interception object communication group's straw-man user, Request distribution of a group session key from said lock management center, and said lock management center, Add a communication terminal of said criminal investigation agency to said communication group, and said communication group's multicast address is given, A key escrow method according to claim 2 removing a communication terminal of said criminal investigation agency from said communication group's member after it sends said group session key to said criminal investigation agency and an interception period expires.

Drawing selection Representative drawing



[Translation done.]

* NOTICES *

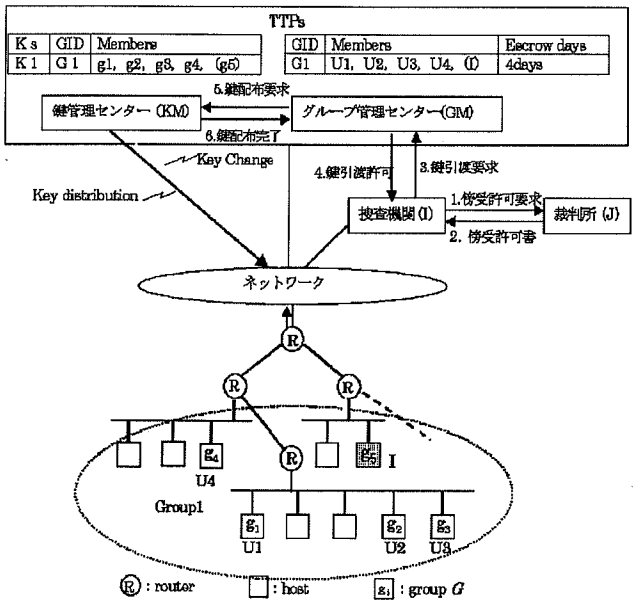
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The figure showing the procedure of the key escrow method in an embodiment of the invention,
[Drawing 2]The figure showing the group session key share sequence of the key escrow method in an embodiment of the invention,
[Drawing 3]The figure showing the session key delivery sequence of the key escrow method in an embodiment of the invention,
[Drawing 4]The key map of the conventional Clipper Chip system,
[Drawing 5]It is an explanatory view of a path definition method and an area definition method in a group cipher communication system.
[Description of Notations]
TTPs Key escrow organization
GM group management center
KM Lock management center
I Criminal investigation agency
J Court

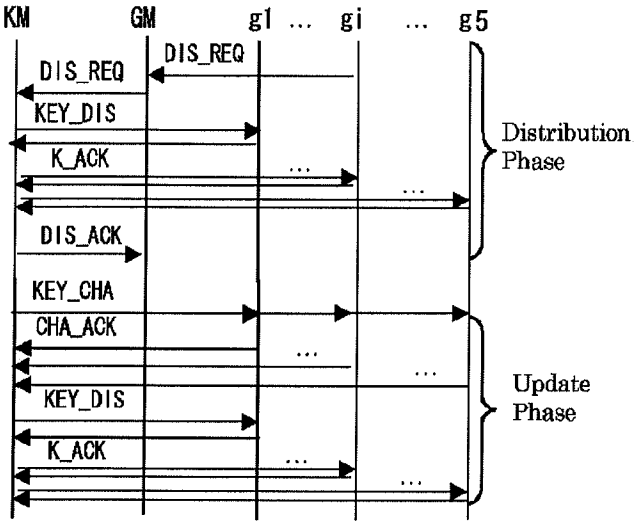
[Translation done.]

Drawing selection Drawing 1



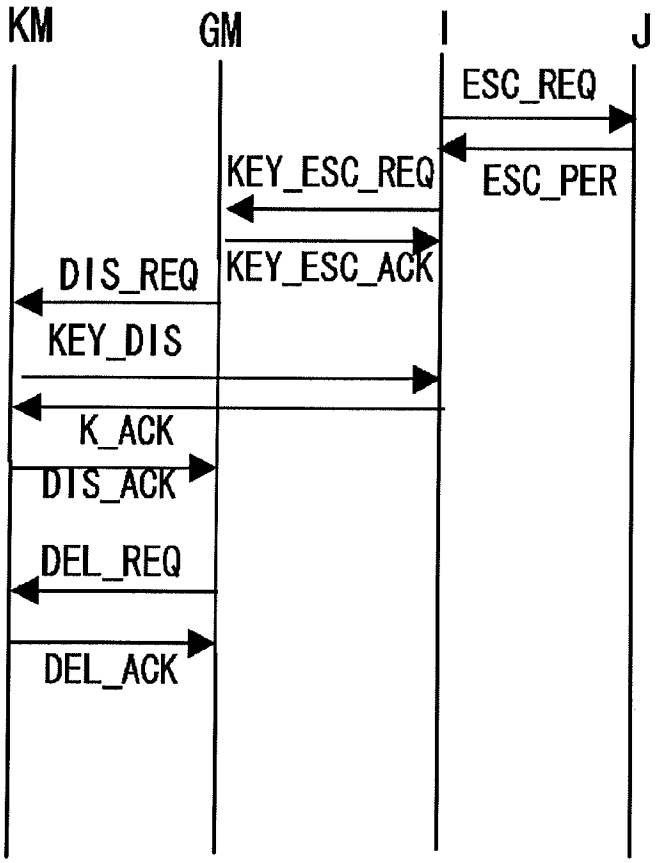
[Translation done.]

Drawing selection Drawing 2



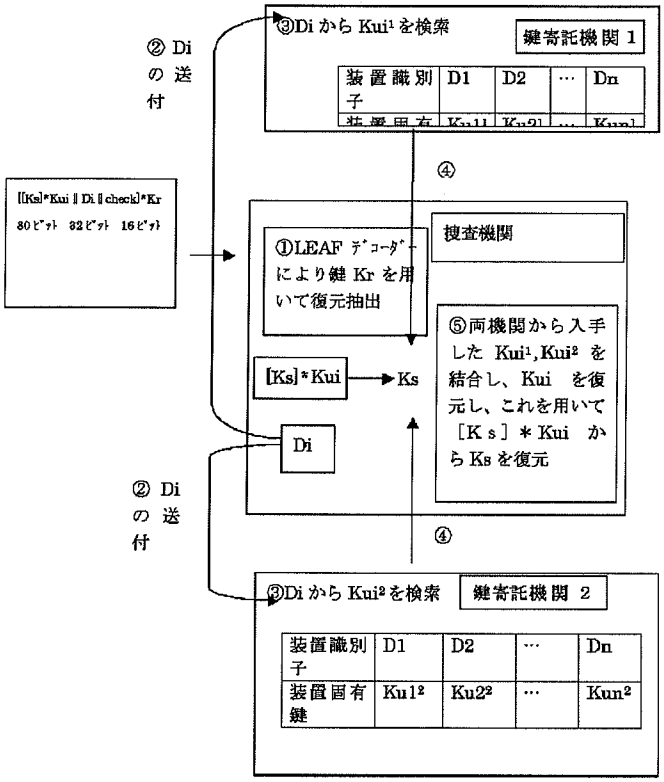
[Translation done.]

Drawing selection Drawing 3



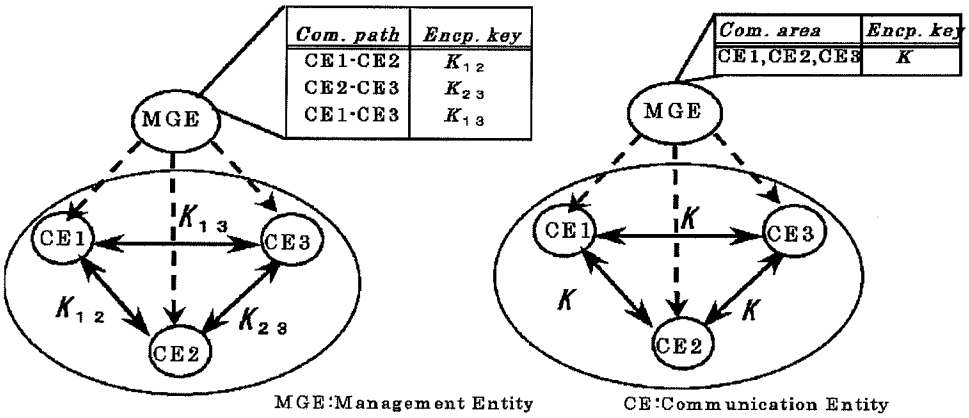
[Translation done.]

Drawing selection Drawing 4



[Translation done.]

Drawing selection Drawing 5



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－211147
（P2001－211147A）
(43)公開日　平成13年８月３日(2001.8.3)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０９Ｃ　1/00	６３０Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６３０		６３０Ｅ	
		Ｈ０４Ｌ　9/00	６０１Ｚ	
			６０１Ｅ	

審査請求　有　　請求項の数３　ＯＬ　（全　８　頁）

(21)出願番号　特願2000－15240(P2000－15240)

(22)出願日　平成12年１月25日(2000.1.25)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

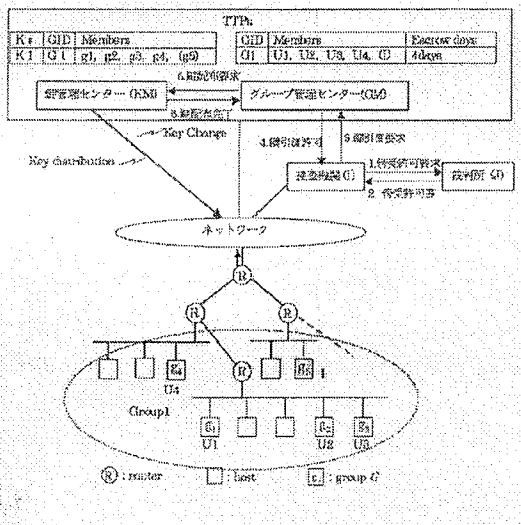
(72)発明者　井上　徹
神奈川県横浜市港北区新横浜三丁目20番地８　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

最終頁に続く

(54)【発明の名称】　キーエスクロー方法

(57)【要約】
【課題】　暗号鍵供託システムを低コストで構成するとともに、捜査機関が傍受開始するまでの時間を短縮する。
【解決手段】　グループセッション鍵を使って暗号通信を行なうグループ暗号通信システムに鍵供託機関を設ける。鍵供託機関でグループセッション鍵を生成配布して通信グループを形成する時に、ダミーユーザーを通信グループのメンバーとして登録する。捜査時には、傍受対象の通信グループのダミーユーザーを捜査機関に割り当てて、暗号通信を傍受して解読する。捜査で必要なときは速やかに通信グループの暗号通信の傍受が可能になり、グループメンバー構成に変化があっても、捜査対象者が含まれる通信グループだけに捜査機関をグループメンバーとして含ませるだけで、確実に暗号通信の傍受ができる。



3

プロトコルであるという点については、誰もがグループアドレスに加わるだけで、マルチキャストパケットを受信できてしまうというセキュリティ上の観点から、大きな問題を有している。例えば、課金を伴うコンテンツ配信サービスなどにおいて、登録メンバー以外にコンテンツを無料で盗み見される可能性がある。また、グループのメンバー以外の者がマルチキャストパケットを送信することができるという問題もある。このような問題を解決して善意のユーザーを保護するために、暗号化グループ通信を行なう必要がある。

【０００９】暗号によりグループ通信を構築する手法としては、図５に示すように、パス定義方式とエリア定義方式がある。図５（ａ）に示すパス定義方式においては、グループメンバーの対毎に異なるセッション鍵を保持し、グループ管理者が、それらをすべて管理する。セッション鍵は、通信セッションの開始時に、通信を行なうグループメンバー間でやり取りされる。この方式では、すべての通信パスが異なる鍵を持つことにより、柔軟なシステムの構築が可能であるが、セッション鍵の管理の負荷が大きく、小規模なシステムに限定される。

【００１０】一方、図５（ｂ）に示すエリア定義方式においては、グループメンバー間で共通のセッション鍵を共有する。セッション鍵は、あらかじめ通信セッションとは独立のタイミングで配布しておく。この方式は、セッション鍵の管理が容易で、大規模なシステムにも適用できる。エリア定義方式によるグループ通信においては、セキュリティの観点から、セッション鍵を定期的に更新する必要がある。また、グループの構成が変化する際にも、セッション鍵の更新が必要になる。

【００１１】このようなマルチキャストルータによって構築されているインターネット上で、暗号化グループ通信を行なうことで、合法的なユーザーを保護する必要がある。それとともに、このような暗号通信システムを悪用することを防ぐために、公権力による傍受を可能にする鍵供託システムを導入する必要がある。

【００１２】クリッパーチップ方式以外の従来の鍵供託方式としては、例えば、R.Ganesan: "Yaksha:Augmenting Kerberos with Public Key Cryptography," Proc. ISOCSymp.on Network and Distributed System Security, Feb.1995.や、山根 義則，櫻井幸一：「無制限な盗聴を防ぐ鍵供託方式」，Proc. SCIS96, Feb.1996.や、高谷和伯，尾形わかは，坂上仁志，高橋豊：「プライバシーを保護する鍵供託方式」，Proc. SCIS99, pp.905-910, Feb.1999.などで提案されているものがある。

【００１３】

【発明が解決しようとする課題】しかし、上記のクリッパーチップ方式では、許可を得てからＬＥＡＦより鍵情報を取り出し、２つの機関に依頼して鍵を合成して、セッション鍵を取り出すので、どうしても２時間以上かかるという問題があった。また、タンパーレジストなハードウェアに依存するため、費用もかかるという問題があった。さらに、偽のＬＥＡＦをつけることにより、傍受を免れうるという問題があった。

4

【００１４】本発明は、上記従来の問題を解決して、グループ暗号通信システムのキーエスクロー方法において、捜査時には捜査機関が低コストで短時間に確実に傍受できるようにすることを目的とする。

【００１５】

【課題を解決するための手段】上記の課題を解決するため、本発明では、グループセッション鍵を使って暗号通信を行なうグループ暗号通信システムのキーエスクロー方法を、鍵供託機関でグループセッション鍵を生成配布して通信グループを形成する時にダミーユーザーを通信グループのメンバーとして登録し、捜査時には、傍受対象の通信グループのダミーユーザーを捜査機関に割り当てて暗号通信を傍受して解読するという構成にした。

【００１６】このように構成したことにより，捜査で必要なときは瞬時に通信グループの暗号通信の傍受が可能になる。また、ダイナミックにグループメンバーが変動する通信ネットワークにおいて、どんなにグループメンバー構成に変化があっても、捜査対象者が含まれる通信グループだけに捜査機関をグループメンバーとして含ませるだけで、確実に暗号通信の傍受ができる。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図３を参照しながら詳細に説明する。

【００１８】本発明の実施の形態は、鍵供託機関でグループセッション鍵を生成配布して通信グループを形成する時に、ダミーユーザーを通信グループのメンバーとして登録し、捜査時には捜査機関にダミーユーザーを割り当てて傍受を行なうキーエスクロー方法である。

【００１９】図１は、本発明の実施の形態におけるキーエスクロー方法の手順を示す概念図である。図１において、ＴＴＰｓ(Trusted Third Parties)は，鍵供託サービスを提供する鍵管理機関である。グループ管理センター（ＧＭ）は、グループメンバーを管理する機関である。鍵管理センター（ＫＭ）は、各グループへのセッション鍵を配布するとともに、定期的にセッション鍵を更新する機関である。捜査機関（Ｉ）は、傍受許可を得て、ＴＴＰｓから鍵を得る捜査機関である。裁判所（Ｊ）は、傍受許可書を発行する裁判所である。

【００２０】図２は、本発明の実施の形態におけるキーエスクロー方法のグループセッション鍵共有シーケンスを示す図である。図２において、ＫＭは、鍵管理センターである。ＧＭは、グループ管理センターである。ｇ１…ｇｉ…は、グループメンバーである。ｇ５は、捜査機関の端末である。

【００２１】図３は、本発明の実施の形態におけるキーエスクロー方法の鍵引渡シーケンスを示す図である。図３において、ＫＭは，鍵管理センターである。ＧＭは、

ンバーリストに関して、マルチキャストアドレス（ＭＡ）を割り当てる。このとき、鍵管理センター（ＫＭ）は、ダミーユーザーないしは捜査機関にもマルチキャストアドレス（ＭＡ）を割り当てる。

【００３４】ＳＴＥＰ２：セッション鍵配布

（２－１）ｇｉ→ＧＭ：ＤＩＳ_ＲＥＱ（Ｇ１）

グループ管理センター（ＧＭ）にグループ登録を行った暗号通信グループのメンバー（ｇｉ）は、図２に示すように、グループ管理センター（ＧＭ）に、グループＩＤのＧ１を付して配布要求を送り、セッション鍵配布を依頼する。

【００３５】（２－２）ＧＭ→ＫＭ：ＤＩＳ_ＲＥＱ（Ｇ１，ＧＬ）

グループ管理センター（ＧＭ）は、鍵管理センター（ＫＭ）に、グループＩＤとグループメンバーリスト（ＧＬ）を付して配布要求を送り、グループへのセッション鍵配布を依頼する。

【００３６】（２－３）ＫＭ→Ｇ：ＫＥＹ_ＤＩＳ［Ｇ１，Ｋ１，time-exp］Ｐｇｉ

鍵管理センター（ＫＭ）は、登録グループＩＤとグループメンバーリストＧＬの確認を行い、メンバーそれぞれに、有効期限付きのセッション鍵（Ｋｓ）としてＫ１を、各ユーザーの公開鍵（Ｐｇｉ）によって暗号化して、ユニキャストで配布する。このセッション鍵（Ｋ１）は有効期限が過ぎると使用しないものとする。

【００３７】（２－４）ｇｉ→ＫＭ：Ｋ_ＡＣＫ（ｇｉ）

自分の秘密鍵（Ｓｇｉ）で復号することにより、有効期限付きのセッション鍵（Ｋ１）を受け取ったグループの各メンバー（ｇｉ）は、鍵管理センター（ＫＭ）にセッション鍵受信応答を返す。

【００３８】（２－５）ＫＭ→ＧＭ：ＤＩＳ_ＡＣＫ（Ｇ１，ＧＬ）

すべてのメンバーからセッション鍵受信応答を受け取ると、鍵管理センター（ＫＭ）は、グループ管理センター（ＧＭ）にセッション鍵配布完了通知を送る。

【００３９】ＳＴＥＰ３：セッション鍵更新

（３－１）ＫＭ→Ｇ：［ＫＥＹ_ＣＨＡ］Ｋ１

鍵管理センター（ＫＭ）は、グループＧ１のマルチキャストアドレス（ＭＡ）宛に、セッション鍵更新メッセージ（ＫＥＹ_ＣＨＡ）を、現在使用しているセッション鍵Ｋ１により暗号化して、ＩＰマルチキャストにより一斉に送信する。

【００４０】（３－２）ｇｉ→ＫＭ：ＣＨＡ_ＡＣＫ（ｇｉ）

各メンバー（ｇｉ）は、鍵管理センター（ＫＭ）に、セッション鍵更新確認応答メッセージを送る。

【００４１】（３－３）鍵管理センター（ＫＭ）は、グループＧ１への新しいセッション鍵を、ＳＴＥＰ２の（２－３），（２－４）に従い再配布する。これを定期的に行なう。

【００４２】図３を参照して、捜査機関が犯罪の疑いのあるグループ暗号通信を傍受するための鍵引渡の手順を説明する。捜査機関が、ある犯罪の可能性があるグループの暗号通信を傍受したい場合、裁判所に傍受許可書を発行してもらわなければならない。裁判所には、捜査機関を認証するために、傍受できる捜査機関を前もって登録しておく。

【００４３】ＳＴＥＰ１：傍受許可要求

１．Ｉ→Ｊ：ＥＳＣ_ＲＥＱ（Ｉ，Ｇ１）

捜査機関（Ｉ）は、自分のＩＤであるＩと、傍受したい犯罪グループの名前であるＧ１を付して傍受要求を送り、裁判所（Ｊ）に傍受許可書発行を要求する。

【００４４】ＳＴＥＰ２：傍受許可書発行

２．Ｊ→Ｉ：ＥＳＣ_ＰＥＲ（$[K_{I,GM}, [LJ]_{KGM}]_{KI}$）

裁判所（Ｊ）は，捜査機関（Ｉ）の認証を行い、正しい捜査機関であったら、傍受有効期間（Ｄａｙｓ）とグループＩＤを定めた証明書付きの傍受許可書（ＬＪ）を発行する。この許可書は、グループ管理センター（ＧＭ）との共通鍵ＫＧＭで暗号化しておく。また、捜査機関（Ｉ）とグループ管理センター（ＧＭ）間で使用できる共通鍵$K_{I,GM}$も用意する。これを捜査機関（Ｉ）との共通鍵ＫＩで暗号化して捜査機関（Ｉ）へ送る。

【００４５】ＳＴＥＰ３：鍵引渡要求

３．Ｉ→ＧＭ：ＫＥＹ_ＥＳＣ_ＲＥＱ（$[A]_{KI,GM}$, $[LJ]_{KGM}$）

捜査機関（Ｉ）は、裁判所（Ｊ）から送られてきた暗号化情報を復号して、グループ管理センター（ＧＭ）との共通鍵（$K_{I,GM}$）と傍受許可書（ＬＪ）を取り出す。そして、自分のＩＤ（Ｉ）、秘密鍵、ホストアドレス（ｇ５）、メッセージ作成時のタイムスタンプを記した自分の認証情報（Ａ）を作成し、これをグループ管理センター（ＧＭ）との共通鍵（$K_{I,GM}$）で暗号化して、グループ管理センター（ＧＭ）に送る。

【００４６】

ＳＴＥＰ４：鍵引渡許可

４．ＧＭ→Ｉ：ＫＥＹ_ＥＳＣ_ＡＣＫ（Ｇ１，Ｄａｙｓ）

グループ管理センター（ＧＭ）は、裁判所（Ｊ）が発行した傍受許可書（ＬＪ）と捜査機関の認証情報を確認した後、捜査機関（Ｉ）を、傍受対象グループＧ１のグループメンバーに追加し、傍受有効期限をタイマー装置で設定し、捜査機関（Ｉ）に傍受期間中の傍受可能である確認応答を示す。

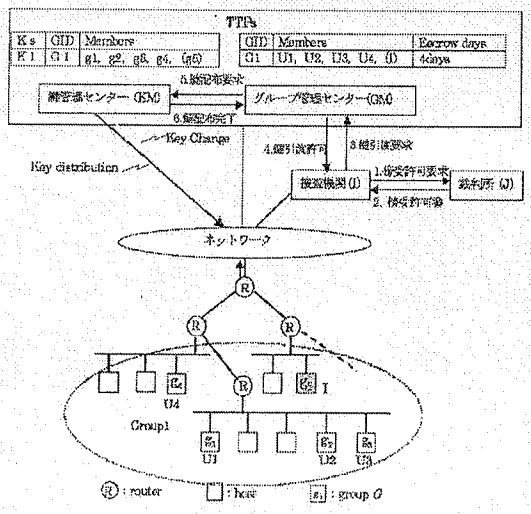
【００４７】ＳＴＥＰ５：グループセッション鍵配布要求

５．ＧＭ→ＫＭ：ＤＩＳ_ＲＥＱ（Ｇ１，ｇ５）

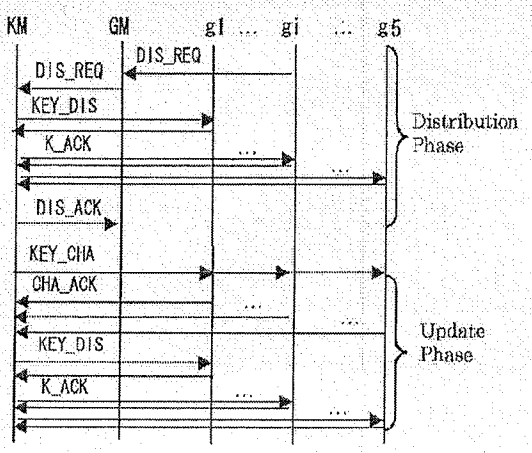
グループ管理センター（ＧＭ）は、鍵管理センター（ＫＭ）に、グループＩＤとグループメンバーＩのホストアドレス（ｇ５）を知らせると共に、そのホストへのセッション鍵配布を依頼する。

【００４８】ＳＴＥＰ６：グループセッション鍵配布

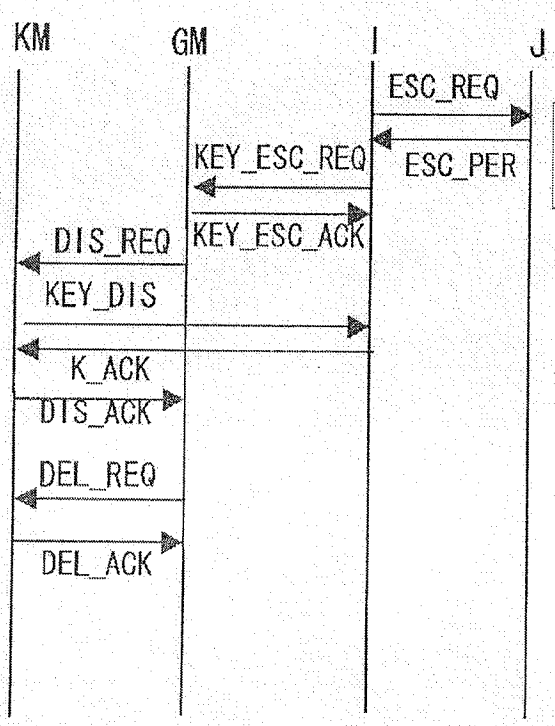
【図１】


TTPs
Ks
KI
GID
GI
Members
g1, g2, g3, g4, ... (g5)
GID
Members
Escrow days
G1
U1, U2, U3, U4, ... (I)
4days
5.鍵配布要求
6.鍵配布完了
鍵管理センター (GM)
グループ管理センター(GM)
Key Change
Key distribution
4.鍵引換許可
3.鍵引換要求
1.鍵受許可要求
2. 鍵受許可通
検索機関 (J)
端末所 (I)
ネットワーク
R
U4
Group1
U1
U2
U3
I
R : router
: host
gi : group G

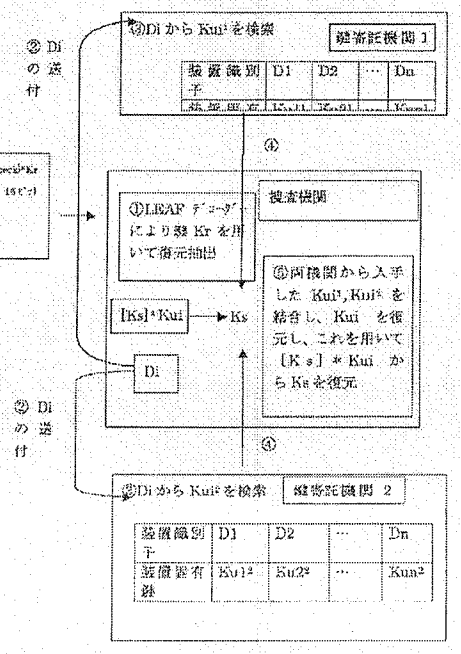
【図２】


KM
GM
g1 ... gi ... g5
DIS_REQ
DIS_REQ
KEY_DIS
K_ACK
DIS_ACK
KEY_CHA
CHA_ACK
KEY_DIS
K_ACK
Distribution Phase
Update Phase

【図３】


KM
GM
I
J
ESC_REQ
ESC_PER
KEY_ESC_REQ
KEY_ESC_ACK
DIS_REQ
KEY_DIS
K_ACK
DIS_ACK
DEL_REQ
DEL_ACK

【図４】


② Di の送付
③Di から Kui² を検索
鍵管託機関 1
装置識別子
D1
D2
…
Dn
④
被盗機関
①LEAF データにより鍵 Kr を用いて復元抽出
③両機関から入手した Kui¹,Kui² を結合し、Kui を復元し、これを用いて【Ks】＊Kui から Ks を復元
【Ks】*Kui
Ks
Di
② Di の送付
③Di から Kui² を検索
鍵管託機関 2
装置識別子
D1
D2
…
Dn
装置署有鍵
Ku1²
Ku2²
…
Kun²